REMARKS/ARGUMENTS

The applicants acknowledge, with thanks, the Office Action dated November 27, 2009. Examiner's withdrawal of the finality of the previous office action is noted with appreciation.

Claims 1, 5, 9-13, 15, 16, and 28-30 have been amended herein. Claims 17-27 were previously canceled. No additional claims have been canceled herein and new claims 31 and 32 have been added. Accordingly, claims 1-16, and 28-30 are currently pending.

The amendments present no new matter. The secure tunnel being established between a server and a peer using an algorithm that establishes a server encryption key possessed by the server and a peer encryption key possessed by the peer is disclosed in the application as published at paragraphs [0008] and [0033] for example. The authenticating the peer with the server establishing a server authentication key possessed by the server and a peer authentication key possessed by the peer is disclosed in the application as published at paragraphs [0010], [0032], and [0033] for example. The network access credential being distributed from the server to the peer responsive to the verifying the peer possesses the same encryption and authentication keys as the server is disclosed in the application as published at paragraphs [0008], [0010], [0033], and [0056] for example. The signaling the authorization failure to the peer in accordance with the distributing of the network access credential is disclosed in the application as published at paragraph [0033] for example.

Reconsideration of the application as amended is respectfully requested.

The Office Action

Claims 1, 9, 28, and 29 were objected to in the Office Action dated November 27, 2009 because, according to the Examiner, there is insufficient antecedent basis for the limitations in each claim. Claims 9-16 were rejected under 35 U.S.C. §101 because, according to the Examiner, the claims are directed to non-statutory subject matter. Claims 1-16 and 28-30 were rejected under 35 U.S.C. §103(a) as being unpatentable over Paul Funk; Simon Blake-Wilson; "draft-ietf-pppext-eap-ttls-02.txt: EAP Tunneled TLS Authentication Protocol (EAP-TTLS)"; Internet-Draft PPPEXT Working Group; Nov. 2002, p. 1-40 (*hereinafter*, "Funk"), in view of US Patent No. 6,397,056 to Bugnon et al. (*hereinafter,* "Bugnon"), and in further view of US Patent

No. RE38,070 to Spies (*hereinafter,* "Spies"). Withdrawal of these rejections is requested in view of the amendments and arguments set forth herein.

The Non-Art Matters

Each of claims 1, 9, 28, and 29 has been amended herein. It is respectfully submitted that the informalities alleged by the Examiner on pages 2 and 3 of the Office Action have each been addressed by these amendments. Accordingly, it is submitted that the claims are improper form.

In addition, independent claim 9 and claims 10-16 dependent therefrom have been amended to recite a system for enabling secure communication between a peer and a server of an associated network. The "implementation" language has been removed from the claims as well. Accordingly, it is submitted that the claims recite statutory subject matter and are in proper form under 35 U.S.C. §101.

The Art Matters

Claims 1-16 and 28-30 were rejected under 35 U.S.C. §103(a) as being unpatentable over Funk in view of Bugnon, and in further view of Spies. Applicants have herein tendered amendments to the claims and it is respectfully submitted that the amended claims are novel, patentably distinct and unobvious over the art of record alone or in combination including Funk, Bugnon, and Spies.

As amended, independent claims 1 and 9 recite a method and system, respectively, for secure communications. A secure tunnel is established between a server of an associated network and a peer using an encryption algorithm that establishes a server encryption key possessed by the server and a peer encryption key possessed by the peer. The peer is authenticated with the server over the secured tunnel establishing a server authentication key possessed by the server and a peer authentication key possessed by the peer. A hashing is made on the server encryption key and the server authentication key to produce a first hash, and a further hashing is made on the peer encryption key and the peer authentication key to produce a second hash. The server verifies that the peer possesses the same encryption and authentication keys as the server by comparing the first hash with the second hash. Responsive to the verifying the peer possesses the same encryption and authentication keys as the server, a network access credential is distributed from the server to the peer using the secured tunnel,. An authorization

failure is signaled to the peer in accordance with the distributing of the network access credential. prior to the peer authenticating with the associated network using the distributed network access credential. The server denies access to the network by the peer until the peer authenticates with the associated network using the distributed network access credential.

The embodiments of the invention provide numerous benefits over the prior art with regard to secure communications and enable a protected dynamic provisioning of credentials from a server to a peer to permit the peer thereafter to authenticate to a network using the provisioned credentials. As described in paragraph [0005] of the application as published:

> A secure tunnel is established between parties using an encryption. The provisioning of credentials is thereafter performed between the parties. An authentication process can be performed between parties over the secured tunnel to ensure proper authorization prior to distribution of said credentials.

In one example embodiment, the Diffie Hellman key agreement is used as the secure key agreement mechanism for establishing the secure tunnel. A secondary authentication mechanism is used to enable the client to prove authenticity by means of different authentication mechanisms for example. The authentication can be any type of authentication mechanism, but in the example embodiment described, Microsoft MSCHAP v2 could be used. The authentication phase within the previously constructed secure tunnel is useful to defend against man in the middle (MitM) attacks, and is intended to provide an indication of unauthorized access control.

In accordance with a further feature of the embodiments of the invention, a further guard against the MitM is in the inclusion of a hashed value that binds the cryptographic results from both the establishment of the secure tunnel (Diffie Hellman key agreement in the example embodiment) and the authentication within the secure tunnel (MSCHAPv2 in the example embodiment) to ensure that both parties (the server 12 and the client 14 in the example embodiment) succeeded in all the message exchanges.

As described at paragraph [0010] in the application as published:

> Further, it should be noted that the present approach can allow for any key exchange mechanism of any method that provides for mutual derivation of

> a shared secret but must guard against MitM attacks. The Diffie Hellman key agreement is chosen as an embodiment as it enables a secure key agreement mechanism; to mitigate possible MitM attacks on Diffie Hellman, this embodiment further enables the use of a server side public/private key pair to be used to sign the DH parameters as a means to authenticate the server. Further, a secondary authentication mechanism is used to enable the client to prove authenticity by means of weaker authentication mechanisms. The authentication can be any type of authentication mechanism, but in the preferred embodiment, Microsoft MSCHAP v2 would be used. The authentication phase is used at present to defend against MitM attacks, and is intended to provide any indication for access control. The final guard against the MitM is in the inclusion of a hashed value that binds the cryptographic results from both the Diffie Hellman key agreement and MSCHAPv2 to ensure that both parties 12, 14 succeeded in all the message exchanges (e.g. M was not present).

It is respectfully submitted that none of the art of record alone or in combination teaches, suggests, or fairly discloses the feature of cryptographically binding the results from both the establishment of the secure tunnel and the authentication within the secure tunnel, wherein the network access credentials are distributed or otherwise provisioned via the secure tunnel after the authorization.

Paragraph [0033] of the application as published describes that, in one example embodiment, the cryptographical binding and the testing therefore are performed using one or more hash functions. As set out there:

> Following a successful MSCHAPv2 authentication exchange, the server and the client must prove that they ensued in both the tunnel establishment and MSCHAPv2 conversations by hashing the resulting keys of both conversations. If both parties prove that they have computed the same hashing result, the server can then provision the peer with a unique credential. Note that any type of credential or set of credentials can be provisioned at this step. On concluding the distribution of the credential or set of credentials, ADHP concludes with an authorization failure, to signal that while credentials have been provisioned, network access is denied until the parties ensue in an actual authentication (versus) provisioning protocol.

Independent claims 1 and 9 include features not disclosed or suggested in the art of record including in particular feature of producing first and second hashes that effectively bind

the results from the secure tunnel formation with those of the authentication within the tunnel. A natural result is to provide assurance that both the server and the peer were the sole participants in the communications and transactions, thereby exposing possible MitM attacks when the hashed values do not match.

More particularly, in the amended independent claims 1 and 9, a secure tunnel is established between a server of an associated network and a peer using an encryption algorithm that establishes a server encryption key possessed by the server and a peer encryption key possessed by the peer. The peer is authenticated with the server over the secured tunnel establishing a server authentication key possessed by the server and a peer authentication key possessed by the peer. A hashing is made on the server encryption key and the server authentication key to produce a first hash, and a further hashing is made on the peer encryption key and the peer authentication key to produce a second hash. The server verifies that the peer possesses the same encryption and authentication keys as the server by comparing the first hash with the second hash.

Turning once again to the Office Action of November 27, 2009, the Examiner took the position that Funk discloses establishing a secure tunnel between a server and a peer using an encryption algorithm that establishes an encryption key, authenticating the peer with the server over the secured tunnel establishing an authentication key, verifying by the server that the peer possesses the same encryption and authentication keys as the server, and provisioning a network access credential to the peer using the secured tunnel, responsive to the verifying the peer possesses the same encryption and authentication keys as the server.

Without conceding the above, applicants respectfully submit that Funk fails to disclose or suggest any connection whatsoever, in a cryptographic sense, between the keys possessed by the server and peer in the secure tunnel establishment and the keys possessed by the server and peer in the authentication. Funk also fails to disclose verifying that the peer possesses the same encryption and authentication keys as the server by comparing first and second hash results based on the encryption and authentication keys. Rather, at most, Funk teaches that during a first phase of negotiation, a TLS handshake protocol is used to authenticate the TTLS server to the client and, optionally, to authenticate the client to the TTLS server, based on public/private key certificates. During a second phase of negotiations in Funk, the client and TTLS server use the secure TLS record layer channel established by the TLS handshake as a tunnel to exchange

information encapsulated in attribute-value pairs, to perform additional functions such as client authentication and key distribution for a subsequent data connection.

In contradistinction, in the amended claims, the secure tunnel establishment and the authentication of the server with the peer are in effect bound in accordance with the network access credential being distributed from the server to the peer using the secured tunnel responsive to the verifying the peer possesses the same encryption and authentication keys as the server by comparing a first hash with a second hash. The first hash is produced by a hashing made on the server encryption key and the server authentication key, and the second hash is produced by a hashing made on the peer encryption key and the peer authentication key. The server verifies that the peer possesses the same encryption and authentication keys as the server by comparing the first hash with the second hash. With regard to the keys in the amended claims, a secure tunnel is established between the server and the peer using an encryption algorithm that establishes a server encryption key possessed by the server and a peer encryption key possessed by the peer. The peer is authenticated with the server over the secured tunnel establishing a server authentication key possessed by the server and a peer authentication key possessed by the peer.

The Examiner has already conceded that Funk is silent on hashing the server encryption key and the server authentication key to produce a first hash, hashing the peer encryption key and the peer authentication key to produce a second hash, verifying by comparing the first hash with the second hash, and signaling an authorization failure to the peer upon conclusion of the provisioning of the network access credential, prior to the peer authenticating using the provisioned credentials, and denying the peer access to the network by the server until the peer authenticates using the provisioned credentials. Applicants agree with the Examiner that Funk is indeed silent in these and further, it is submitted that neither Spies nor Bugnon disclose any teachings which would remedy the deficiencies of Funk.

In particular, although the Examiner took the position with regard to Spies that "using hash function during authentication process is well known in the art," applicants respectfully submit that the manner in which the hash function is used in Spies is different than the manner in which it is used and claimed in the subject application. In Spies, in general, a sender of information sends the information together with a hash value calculated on that information. A receiver in turn receives the information and calculates its own hash value which is then

compared against the hash value provided by the sender. The Examiner's citation to column 9, lines 24-36 of Spies is instructive and supports applicants' remarks wherein:

> the participant's private key of the signing pair was employed to perform the encryption. By encrypting the participant's signature with its own private signing key, the eventual recipient will be able to verify the participant's digital signature by decrypting the hash using the participant's public signing key, independently computing the hash of the original message, and comparing the locally computed hash with the decrypted hash. The comparison will succeed only if the participant's private signing key was used to encrypt the hash. Since only the originating participant knows the private signing key, the recipient knows that the originating participant actually created the encrypted hash, essentially "signing" the document.

On the other hand, in the claims, the first hash is based on the server encryption key and the server authentication key. Unlike the teachings of Spies, the second hash in the claims is not based on the server encryption key and the server authentication key for a comparison against the first hash based on the same underlying information, but rather the second hash in the claims is based on the peer encryption key and the peer authentication key.

In addition to the above, it is respectfully submitted that Bugnon does not cure the deficiencies of either Funk or Spies. Bugnon was cited for its alleged teaching of the concept of sending authentication failure messages until a positive authentication is made. However and without conceding the Examiner's understanding of Bugnon, in the amended claims, the authorization failure is signaled to the peer in accordance with the distributing of the network access credentials. In the claims, the network access credentials are distributed from the server to the peer responsive to a verifying that the peer possess the same encryption and authentication keys as the server.

Thus, contrary to the Examiner's position with regard to Bugnon in the Office Action. The teachings thereof are not useful in curing the deficiencies of Funk and/or Spies.

In accordance with the above, therefore, it is respectfully submitted that neither Funk nor Bugnon or Spies, alone or in combination teach, suggest or fairly disclose the embodiments recited in the amended claims.

CONCLUSION

In accordance with the afore-noted amendments and comments, withdrawal of the rejections to this application is requested and a Notice of Allowance is earnestly solicited. If there are any fees necessitated by the foregoing communication, the Commissioner is hereby authorized to charge such fees to our Deposit Account No. 50-0902, referencing our Docket No. 72255/00006.

Respectfully submitted,

Date: 7-27-10

Larry B. Donovan
Registration No. 47,230
TUCKER ELLIS & WEST LLP
1150 Huntington Bldg.
925 Euclid Ave.
Cleveland, Ohio 44115-1414
Customer No.: 23380
Tel.: (216) 696-3864
Fax: (216) 592-5009